

MSC Guidelines for Review of Design Verification Test Procedures

Procedure Number: E2-5

Revision Date: 04/20/00

References:

- a. Title 46 CFR Titles 58, 61 and 62
- b. Title 46 CFR Parts 111 and 112
- c. Navigation and Inspection Circular (NVIC) 2-89, "Guide for Electrical Installations on Merchant Vessels and Mobile Offshore Drilling Units"
- d. American Bureau of Shipping (ABS), "Rules for Building and Classing Vessels under 90 Meters in Length", 1996
- e. Safety Of Life at Sea (SOLAS), Consolidated Editions, 1997, Chapter II-1, Part D
- f. MSC Procedures E2-1, Vital System Automation and E2-18, Qualitative Failure Analysis.

Disclaimer

These guidelines were developed by the Marine Safety Center staff as an aid in the preparation and review of vessel plans and submissions. They were developed to supplement existing guidance. They are not intended to substitute or replace laws, regulations, or other official Coast Guard policy documents. The responsibility to demonstrate compliance with all applicable laws and regulations still rests with the plan submitter. The Coast Guard and the U. S. Department of Transportation expressly disclaim liability resulting from the use of this document.

Contact Information

If you have any questions or comments concerning this document, please contact the Marine Safety Center by e-mail or phone. Please refer to the Procedure Number:

E2-5

E-mail: customerservicemsc@uscg.mil

Phone: 202-366-6480.

Applicability

- Applicable to self-propelled vessels of 500 gross tons and over that are certificated under subchapters D, I, and U, and to self-propelled vessels of 100 gross tons and over that are certificated under subchapter H.
- The Design Verification Test Procedure (DVTP) document is required to be "**Approved**" and retained aboard the vessel. Using the DVTP document, design verification testing is required to be performed immediately after the installation of the automated equipment or before the issuance of the initial Certificate of Inspection. Final approval of the DVTP document is contingent upon satisfactory completion of onboard design verification tests in the presence of the Coast Guard. See 46 CFR 61.40-1(c), and 62.30-10(a).

MSC Guidelines for Review of Design Verification Test Procedures

Procedure Number: E2-5

Revision Date: 04/20/00

General Review Guidance

- Design verification testing is used to verify the automated vital system installations are designed, constructed and operate in accordance with the applicable requirements in 46 CFR Part 62. See 46 CFR 61.40-3.
- The design verification test procedures may be incorporated with the qualitative failure analysis (QFA). See procedure number E2-18.
- The DVTP document is a separate document from the Periodic Safety Test Procedure (PSTP) document. Both documents are required to be approved and retained aboard the vessel. See 46 CFR 61.40-1(c).
- The DVTP document, if submitted separately with the QFA document, must include the following QFA document information:
 - a. Component Failure Considered
 - b. Failure Effects
 - c. Failure Detection
 - d. Alternatives or Control Alternatives Available to the Crew

See Attachments 1 and 2 for sample DVTP formats.

- Examine the test instructions to insure that they closely or realistically simulate the failure of only the failed component of each of the failures considered in the failure analysis. For example: A PLC power supply module failure may be tested by removing the fuse to the power supply module, but a CPU failure (served by the same power supply module), should not be tested using the same power supply fuse, as it is desired that the power supply remain in operation, with just the CPU failing.
- Test instructions should be prepared as if the vessel is underway, in pilothouse automatic pilothouse control, various machinery automation in normal underway mode of operation, and the engineroom manned to the manning level design of the machinery plant.
- Design verification testing using the failures considered in the QFA should consider the vital system automation installation as an integrated system, although as a whole it may be comprised of different components supplied by various manufacturers. In other words, various automated systems, although supplied by separate manufacturers, may be used to monitor the operational integrity of other systems and provide failure alarms.

MSC Guidelines for Review of Design Verification Test Procedures

Procedure Number: E2-5

Revision Date: 04/20/00

- Programmable control or alarm system logic must not be altered after satisfactory completion of Design Verification Tests without the approval of the cognizant Officer in Charge, Marine Inspection. This comment should be included in the approval letter of the DVTP document to insure the cognizant OCMI and the ship's owner are aware of the requirements. See 46 CFR 62.25-25(a). This means that the DVTP document is only used during the initial issuance of the vessel's certificate of inspection or immediately after the installation of the automated equipment, and when the installed automated equipment is upgraded or altered. For the PSTP document, periodic safety testing is conducted at periodic intervals specified by the Coast Guard.

Attachments:

1. Sample A, DVTP Format
 2. Sample B, DVTP Format
-

MSC Guidelines for Review of Design Verification Test Procedures

Procedure Number: E2-5

Revision Date: 04/20/00

1.4 6032-610 Digital Input Board Failure

- Effect on the system
Input channels for failed board are no longer updated (32 channels).
- Failure detection
NO board failure LEDs on the 6032-610 board and on the communication processor are illuminated. Diagnostic alarm message 6032 board position XX failure appears on local operator panels and on graphic workstations. XX indicates the position of the card in the computer rack.
- Failure recovery
Replace failed 6032-610 board.
- Failure simulation
Withdraw 6032-610 from rack.

1.5 6001-610 Communication Processor Board Failure

- Effect on the system
Graphic work stations and local operator panels are no longer updated. Alarm conditions are still indicated on the front panel of the system in the engine control room.
- Failure detection
Processor board failure LED on 6001-610 board is illuminated. Diagnostic alarm message "CAM XX disconnected" appears on the graphic workstations. Green "system on" LEDs on local operator panels are no longer illuminated.
- Failure recovery
Replace failed 6001-610 board.
- Failure simulation
Withdraw 6001-610 from rack.

1.6 Duty Selection Unit Failure

- Effect on the system
No longer possible to select a duty engineer or to create a general engineers alarm.
- Failure detection
Diagnostic alarm message "duty selection unit failure" appears on the local operator panels and on the graphic workstations. Green "system on" LED on duty selection unit is no longer illuminated.
- Failure recovery
Check the power fuse on the back of the unit and if the feed wires are properly connected. Replace failed duty selection unit.
- Failure simulation
Remove power fuse from the duty selection unit.

Sample A, DVTP Format

MSC Guidelines for Review of Design Verification Test Procedures

Procedure Number: E2-5

Revision Date: 04/20/00

1B4 Loss of Control Interface Slave Module

Testing the failure effects on the starboard boiler combustion control process.

WARNING: Removal of the IMCIS02 in Step 1 below will cause the starboard boiler to go to low fire due to the fuel oil control valve failing.

STEP	COMPONENT	ACTION	RESULT	ALTERNATE ACTION/CONTROL	ALARM	VERIFIED
1	IMCIS02 PCU 1 Module 2 Slave 1	In PCU Cabinet #1, remove the IMCIS02 module with the address Module 2 Slave 1.	Analog inputs to the INFI 90 System from this module show last known value as 'bad quality'. Analog outputs from the module go to 0 volt.		System alarm Bad Quality Indicated for Inputs to this module	—
			The starboard boiler goes to low fire due to the fuel oil control valve failing to minimum due to loss of control signal.	If the starboard boiler must be operated, manual control can be maintained from the ISSAC in the by pass mode. Also manually control low valve via the valve hand wheel.	Starboard Boiler Trip Alarm	—
			The starboard boiler alarm low signal is lost. The steam drum level should not be corrupted in automatic without the signal.	If the starboard boiler must be operated, drum level must be controlled by the ISSAC in the by pass mode.		—
			The starboard superheated temperature control valve fails open due to loss of control signal.	If the starboard boiler is operated, the superheater control valve must be operated by the ISSAC in the by pass mode or in Local Manual Control.		—
2	IMCIS02	In PCU #1 insert the IMCIS02 module which was removed in Step 1 above with the address Module 2 Slave 1.	Functions and control test in Step 1 above are restored. System is normal.			—

Sample B, DVTP Format